DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
D. L.VO 196/2003

1. Principi generali

Il presente Documento Programmatico sulla Sicurezza (D.P.S.) costituisce una misura minima di sicurezza inerente il trattamento con strumenti elettronici dei dati personali sensibili e giudiziari. Il D.P.S. contiene informazioni e prescrizioni in base a quanto previsto dal D. L.vo 196/2003, compreso l'Allegato B (All. B) "Disciplinare tecnico in materia di misure minime di sicurezza". Le prescrizioni sono estese ai trattamenti di dati personali effettuati con qualsiasi strumento.

Attraverso le prescrizioni contenute nel D.P.S. l'Ente persegue i seguenti obiettivi:
1. ottemperanza agli adempimenti stabiliti da norme giuridiche o da provvedimenti emanati dalle Autorità competenti;
2. diffusione della cultura della protezione delle risorse produttive;
3. evidenziazione dell'importanza strategica e del valore delle informazioni;
4. razionalizzazione ed ottimizzazione dell'organizzazione, delle funzioni, dei processi e delle attività;
5. uniformità dei principi di trattamento delle informazioni e dei dati;
6. incentivazione al decentramento operativo;
7. efficacia dei processi e delle attività trasversali alla struttura;
8. valorizzazione e responsabilizzazione del personale;
9. formazione permanente del personale.

In base alle caratteristiche della struttura e dell'organizzazione dell'Ente, descritte nel Regolamento di Organizzazione, alle attività istituzionali svolte ed ai compiti e responsabilità dei Dirigenti, il D.P.S. indica i criteri programmatici cui i Dirigenti, così come individuati al punto 4.1, in qualità di Responsabili dei trattamenti, devono attenersi per garantire la protezione dei dati. Tale impostazione riflette l'articolazione dell'Ente in strutture operative connotate da specificità tali da non consentire la definizione di modalità standardizzate o centralizzate per quanto concerne il trattamento dei dati personali.

L'attuazione delle prescrizioni contenute nel D.P.S. è basata sul principio della documentazione e della certificazione. Tutte le attività svolte per garantire la sicurezza dei dati personali devono essere svolte secondo procedure la cui conformità alle linee guida dell'Ente, contenute nel D.P.S. o in altri atti, viene verificata dal Titolare, attraverso l'Unità Organizzativa Gabinetto del Sindaco.

2. Definizioni

Il presente D.P.S. recepisce le definizioni contenute nell'articolo 4 del D. L.vo 196/2003, introducendone di nuove e apportando altresì alcune semplificazioni.

Ai fini della corretta interpretazione del documento, si intende per:
Dato ultrasensibile: dato personale sensibile idoneo a rivelare lo stato di salute o la vita sessuale.
Minaccia: un potenziale evento dannoso conosciuto.
Obiettivo di Intervento (O.I.): il contesto fisico o logico, ovvero l'oggetto su cui vengono applicate

le misure di sicurezza.
Rischio: la probabilità di accadimento di una minaccia.
Sicurezza: l'integrità, la riservatezza e la disponibilità dei dati.
Sistema informatico: il sistema di gestione automatizzata delle informazioni nell'ambito di un'organizzazione.
Sistema informativo: il sistema di gestione di tutte le informazioni nell'ambito di un'organizzazione.
Supporto di trattamento: l'elemento materiale su cui vengono trattati e trasmessi i dati.
Vulnerabilità: l'attitudine intrinseca di una risorsa a subire gli effetti della realizzazione di una minaccia.

3. Informazioni sull'elenco dei trattamenti dei dati personali (All. B - 19.1)

3.1 Elenco delle banche di dati

Il Responsabile redige l'elenco delle banche di dati personali di competenza e ne cura la conservazione e l'aggiornamento.

Ad ogni banca di dati viene attribuito un codice che indica:
-la sua identità;
-l'eventuale soggetto esterno, diverso dall'interessato, da cui si acquisisce;
-il soggetto interno che la detiene.

L'elenco, per ogni banca di dati, deve indicare:
-il codice di identità;
-l'ubicazione;
-i riferimenti documentali circa il contenuto della banca di dati;
-l'interconnessione con altre banche di dati.

3.2 Elenco dei trattamenti

Il Responsabile redige l'elenco dei trattamenti di dati personali di sua competenza e ne cura la conservazione e l'aggiornamento.

Ad ogni trattamento viene attribuito un codice che indica la sua identità.

L'elenco, per ogni trattamento e con riferimento ai compiti degli incaricati, deve indicare:
-la sua identità;
-l'identità della banca di dati in cui il dato trattato è registrato;
-il tipo di dato trattato;
-l'obiettivo del trattamento;
-il presupposto giuridico del trattamento;
-la descrizione sintetica del trattamento;
-le operazioni eseguibili;
-gli uffici abilitati al trattamento;
-gli eventuali soggetti esterni incaricati del trattamento;
-i soggetti cui i dati devono essere eventualmente comunicati;
-gli strumenti impiegati per il trattamento.

4. Informazioni sulla distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati (All. B - 19.2)

4.1 Figure preposte al trattamento e altre figure

Titolare del trattamento dei dati personali è la Civica Amministrazione, nella persona del Sindaco pro tempore.

Responsabili interni del trattamento dei dati personali sono il Direttore Generale, il Vice Direttore Generale, i Direttori, il Capo di Gabinetto, i Dirigenti Responsabili delle Unità Organizzative del Segretario Generale e del Direttore Generale, i Dirigenti Responsabili delle Unità di Progetto, i Dirigenti Responsabili delle Divisioni Territoriali, ciascuno per quanto concerne la struttura di competenza.

Gli Incaricati del trattamento dei dati personali sono le persone fisiche designate dai Responsabili ad effettuare trattamenti di dati personali.

I Referenti sono le persone fisiche designate dai Responsabili per svolgere le funzioni di cui al punto 4.4.

Il "Gruppo di lavoro per l'applicazione della normativa sulla protezione dei dati personali" viene istituito con provvedimento del Sindaco per svolgere le funzioni di cui al punto 4.5.

4.2 Compiti del Titolare

Il Titolare:

- -nomina i Responsabili, interni ed esterni, del trattamento.
- -informa tempestivamente i Responsabili, tramite il "Gruppo di lavoro per l'applicazione della normativa sulla protezione dei dati personali", circa le variazioni delle norme in materia di trattamento di dati personali, nonché in merito alle regole che definiscono i compiti degli stessi;
- -assume, su proposta dei Responsabili, le decisioni in ordine alle finalità del trattamento, ivi compreso il profilo della sicurezza;
- -acquisisce le relazioni annuali dei Responsabili circa i trattamenti effettuati;
- -effettua, attraverso l'Unità Organizzativa Gabinetto del Sindaco, controlli sull'operato dei Responsabili, anche verificando la conformità al D.P.S. delle procedure adottate;
- -coordina l'applicazione delle misure di sicurezza;
- -emana annualmente il D.P.S. ed eventuali allegati.

4.3 Compiti dei Responsabili

Il Responsabile:

- -individua le norme di legge o di regolamento, ovvero i fini istituzionali o le rilevanti finalità di interesse pubblico, in base ai quali deve o può essere effettuato un trattamento di dati personali;
- -formula proposte al Titolare circa le decisioni da assumere in ordine alle finalità del trattamento, ivi compreso il profilo della sicurezza;
- -effettua le comunicazioni e realizza gli altri adempimenti previsti dalla normativa vigente nei confronti del "Garante per la Protezione dei Dati Personali" o di altri organismi ispettivi;
- -istituisce e gestisce le banche di dati di competenza, redigendone l'elenco;

-classifica i dati in base alla loro tipologia, nel momento in cui vengono acquisiti o generati, ovvero ne viene modificata la struttura in seguito a trattamento;
-individua i trattamenti di competenza, redigendone l'elenco;
-stabilisce le procedure e le modalità di effettuazione dei trattamenti, individuando gli strumenti utilizzabili;
-predispone la scheda per l'informativa ed attua tutti gli accorgimenti per garantire l'esercizio dei diritti dell'interessato;
-individua i luoghi fisici in cui sono allocate le banche di dati ed in cui vengono effettuati i trattamenti;
-individua gli Obiettivi di Intervento (O.I.);
-effettua l'Analisi dei Rischi (A.R.);
-ottempera alle disposizioni del D.P.S.;
-adotta le misure minime di sicurezza previste dalla norma e tutti gli altri accorgimenti necessari per prevenire la distruzione, la perdita o l'alterazione dei dati, l'accesso ed i trattamenti non autorizzati o non conformi alle finalità del trattamento, nonché per assicurarne la disponibilità ai fini del trattamento e per garantire l'esercizio dei diritti dell'interessato;
-definisce i profili degli Incaricati in base alla necessità di accedere ai dati e di effettuare i trattamenti;
-nomina per iscritto gli Incaricati, in base alle funzioni ed ai trattamenti effettuati dagli uffici;
-nomina almeno un Referente per la protezione dei dati personali;
-definisce i programmi di formazione degli Incaricati, secondo i principi espressi nel D.P.S.;
-effettua controlli sui trattamenti di competenza, compresi quelli esternalizzati;
-comunica tempestivamente al Titolare situazioni di criticità o di rischio a carico dei dati personali e dei trattamenti di competenza;
-elabora, entro il 31 Gennaio di ogni anno, una relazione riferendo al Titolare in merito alla gestione dei dati personali effettuata dalla struttura di competenza nel corso dell'anno precedente e formulando, se del caso, osservazioni e proposte;
-collabora alla definizione dei provvedimenti del Titolare in materia di trattamento dei dati, ivi compresa la nomina di Responsabili di trattamento esterni all'Ente;
-individua e nomina per iscritto i soggetti esterni Incaricati di trattamento e definisce modalità e standard, sia tecnici che organizzativi, per l'effettuazione dei trattamenti medesimi, accertando che le prescrizioni siano formalmente accettate e sostanzialmente applicate dai soggetti esterni;
-stabilisce i casi in cui i dati devono essere comunicati, nonché le relative modalità di comunicazione;
-concorda formalmente, in caso di trattamento congiunto con strutture interne facenti capo ad altri Responsabili, procedure, modalità di trattamento, strumenti utilizzabili, operazioni eseguibili e misure di sicurezza, sulla base delle competenze attribuite dall'Amministrazione alle singole strutture;
-attua quanto non sia espressamente previsto dal presente D.P.S. al fine di garantire la puntuale applicazione della normativa in materia di trattamento e protezione dei dati personali.

4.4 Compiti dei Referenti

Il Referente:
-svolge attività di consulenza alla struttura di appartenenza;
-svolge, su delega del Responsabile, attività di coordinamento all'interno della struttura di competenza;
-effettua interventi di formazione interna;
-mantiene rapporti con il "Gruppo di lavoro per l'applicazione della normativa sulla protezione dei dati personali", facendo da tramite tra quest'ultimo ed il Responsabile di riferimento.

4.5 Compiti del "Gruppo di lavoro per l'applicazione della normativa sulla protezione dei dati personali"

Il "Gruppo di lavoro per l'applicazione della normativa sulla protezione dei dati personali":

- -informa tempestivamente i Responsabili, attraverso i Referenti, circa le variazioni delle norme in materia di trattamento di dati personali, nonché in merito alle regole che definiscono i compiti degli stessi;
- -collabora con i Responsabili o altri soggetti alla predisposizione di atti dell'Ente;
- -effettua attività di consulenza all'interno dell'Ente;
- -mantiene rapporti con i Referenti e, tramite questi, con i Responsabili;
- -contribuisce a pianificare gli interventi di formazione nei casi previsti al punto 8.

5. Informazioni sull'Analisi dei Rischi (All. B - 19.3)

L'Analisi dei Rischi (A.R.) ha natura dinamica e permanente. Viene predisposta al fine di mettere in relazione le risorse da proteggere, i rischi da cui sono interessate e le misure di sicurezza da adottare.

L'A.R. viene obbligatoriamente effettuata negli stessi casi in cui è obbligatorio procedere con la formazione degli Incaricati (8).

L'A.R. dei rischi prevede:

1. la classificazione del dato;
2. la valutazione del dato in base alla sua criticità (giuridica, economica, produttiva, immateriale);
3. la contestualizzazione del dato all'interno dell'architettura del sistema informativo, con principale riferimento alla sua localizzazione, elaborazione e comunicazione/trasmissione;
4. la definizione degli O.I. e della loro vulnerabilità;
5. l'individuazione delle minacce di cui sono oggetto gli O.I.;
6. l'analisi delle possibili modalità di accadimento delle minacce, in base alla loro natura (accidentale, colposa o dolosa) e origine (esterna o interna);
7. la considerazione e la misurazione delle conseguenze in caso di accadimento dell'evento dannoso;
8. la definizione, su base probabilistica, del livello di rischio;
9. la definizione di una scala di priorità in merito all'adozione di misure di sicurezza.

6. Informazioni sulle misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità (All. B - 19.4)

Le misure di sicurezza vengono applicate al fine di garantire l'integrità, la disponibilità e la riservatezza dei dati, con particolare riguardo alla prevenzione.
Per ogni O.I., individuato in base alla posizione fisica e logica delle banche dati e dei trattamenti nell'ambito del sistema informativo, devono essere indicati, conseguentemente all'effettuazione dell'A.R.:

- -il codice della banca di dati;
- -il codice del trattamento;
- -la tipologia della misura adottata (tecnica, informatica, organizzativa, logistica, procedurale);

-gli strumenti e le procedure adottate, nonché gli scopi perseguiti;
-la stima del rischio residuo.

Ogni O.I. può comprendere più banche di dati e trattamenti. La protezione dell'O.I. deve essere ottimizzata al fine di perseguire congiuntamente la sicurezza delle persone e delle risorse materiali e immateriali a fronte di minacce di natura accidentale, colposa o dolosa, nonché di origine interna o esterna.

7. Informazioni su criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento (All. B - 19.5)

Il Responsabile garantisce la disponibilità dei dati adottando misure idonee per la loro duplicazione e per il ripristino delle banche di dati.

I criteri e le modalità per il ripristino della disponibilità dei dati, considerata l'Analisi dei Rischi, sono riferiti a:

-idoneità delle strutture (rispetto delle destinazioni d'uso, adeguamento, compartimentazione, fruizione, gestione delle attività, gestione degli accessi);
-adozione di procedure per il controllo degli accessi alle risorse fisiche e logiche, per la duplicazione dei dati, per il ripristino delle banche di dati e, nei casi in cui è possibile, per la rigenerazione dei dati;
-adozione di procedure per la duplicazione, informatizzata o mista, dei dati, nonché per la custodia separata delle banche di dati;
-acquisizione, gestione e aggiornamento di tecnologie e di strumenti per il ripristino delle banche di dati;
-controllo e manutenzione dei supporti di memoria e degli strumenti di trattamento.

8. Informazioni sulla previsione degli interventi formativi degli Incaricati (All. B - 19.6)

I Responsabili, di concerto con gli Uffici dell'Ente preposti alla formazione del personale, organizzano gli interventi formativi per gli Incaricati di trattamento ed i Referenti.

Gli interventi di formazione, limitatamente al personale interessato, sono obbligatori nei seguenti casi:

-modificazione o integrazione della normativa di riferimento (*);
-modificazione o integrazione delle norme dell'Ente (*);

-variazione della struttura organizzativa dell'Ente;
-ridefinizione delle competenze delle Direzioni e delle strutture subordinate;
-adozione di nuove procedure per la sicurezza dei dati (*);
-variazioni interne di una struttura;
-assunzione di personale (*);
-passaggio di categoria;
-variazione di qualifica;
-trasferimento ad altro Ufficio;
-assegnazione ad altro incarico o mansione;

-istituzione di nuovi trattamenti;

-variazione o aggiornamento dei trattamenti;
-istituzione di nuove procedure;
-variazione o aggiornamento di procedure;
-adozione di nuovi strumenti di trattamento;
-adozione di nuovi strumenti per la sicurezza dei dati (*).

Gli interventi di formazione sono improntati al principio del più ampio decentramento, attraverso l'ausilio dei Referenti. Nei casi contrassegnati con l'asterisco (*), data la trasversalità delle materie, la formazione viene pianificata con il contributo del "Gruppo di lavoro per l'applicazione della normativa sulla protezione dei dati personali".

Il Responsabile predispone il piano di formazione e registra i corsi di formazione effettuati, dandone conto al Titolare. Nel caso in cui non ricorrano i presupposti per effettuare interventi di formazione, il Responsabile effettua opera di sensibilizzazione del personale, per iscritto e con cadenza almeno semestrale, richiamando i principi cui si ispira la normativa in materia, i provvedimenti delle Autorità competenti, le regole dell'Ente e le prescrizioni contenute nel presente Documento Programmatico sulla Sicurezza.

9. Informazioni sui criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al Codice, all'esterno della struttura del Titolare (All. B - 19.7)

Nel caso di trattamenti affidati all'esterno della struttura del Titolare, il Responsabile inserisce nel Capitolato Speciale le clausole indicanti le direttive cui il soggetto esterno deve attenersi, specificando l'obbligo di conformità a quanto previsto nel presente D.P.S.. Le clausole devono prevedere l'obbligo di adottare autonomamente le misure minime di sicurezza previste dalla normativa vigente. Le clausole devono evidenziare la facoltà dell'Ente di effettuare controlli, a seguito dei quali possono essere applicate penali ovvero può essere risolto il contratto. In base all'A.R., il trattamento effettuato dal soggetto esterno deve garantire lo stesso livello di sicurezza previsto per lo stesso tipo di dati trattati all'interno.

1.Informazioni sui criteri da adottare per la cifratura o la separazione dei dati personali idonei a rivelare lo stato di salute e la vita sessuale (dati ultrasensibili) dagli altri dati personali dell'Interessato (All. B - 19.8)

Il Responsabile, con riguardo ai dati personali sensibili idonei a rivelare lo stato di salute e la vita sessuale dell'Interessato, individua le banche di dati ed i relativi trattamenti. Redige procedure per limitare i trattamenti ai soli casi indispensabili per lo svolgimento delle funzioni istituzionali e per gli adempimenti previsti da leggi o da regolamenti. Individua gli Incaricati del trattamento e ne descrive analiticamente i compiti, in base alle operazioni autorizzate. Disciplina l'accesso ai dati da parte degli Incaricati, sulla base del principio della "necessità di sapere" e del "minimo privilegio".
In caso di trattamento informatizzato, il Responsabile utilizza gli strumenti applicativi necessari per crittografare i dati sensibili idonei a rivelare lo stato di salute e la vita sessuale.
In caso di trattamento cartaceo, provvede a separare fisicamente e a custodire separatamente i dati personali da quelli ultrasensibili. All'Interessato viene abbinato un codice identificativo che consenta di unificare le informazioni contenute in archivi separati. Nei documenti contenenti dati sensibili idonei a rivelare lo stato di salute e la vita sessuale l'Interessato è individuabile solamente mediante il codice sopra menzionato.